UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/037,153	12/21/2001	Chui-Shan Teresa Lam	09469.010001	5605

22511 7590 03/29/2006

OSHA LIANG L.L.P.
1221 MCKINNEY STREET
SUITE 2800
HOUSTON, TX 77010

EXAMINER	
HEWITT II, CALVIN L	
ART UNIT	**PAPER NUMBER**
3621	

DATE MAILED: 03/29/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/037,153	LAM ET AL.	
	Examiner	Art Unit	
	Calvin L. Hewitt II	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 January 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,11-20,22,23 and 25-35* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,11-20,22,23 and 25-35* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Status of Claims

1. Claims 1-9, 11-20, 22, 23, and 25-35 have been examined.

Response to Amendment/Arguments

2. Applicant is of the opinion that the prior art does not teach a memory storing data in a n-tuple wherein the n-tuple comprises a key name, key value and key type field. The Examiner respectfully disagrees. Auerbach et al. disclose a Bill of Materials database comprising fields (figure 3). One entry in the database is an encryption key denoted in a field as "ENCRYPTED PEK 3". This information conveys to one of ordinary skill the name of the key "ENCRYPTED PEK 3" and the type "PEK 3" (i.e. part encryption key of part 3). In the next column, the BOM provides a field containing the signature of the key or "value". Hence, Auerbach et al. provide a key name, key value and key type field as the claims are silent regarding the fields being distinct. Nonetheless, it has been held that it would have been obvious to one of ordinary skill to arrange (*In re Seid*, 73 USPQ 431 (CCPA 1947)) the data in the database such the content (e.g. abstract, encrypted parts, terms for using said parts) is separate from the keys such as by creating a second "key" database and using whatever data descriptors a programmer deems appropriate for describing the data (e.g. "key

id", "corresponding part", and "signature" fields) (*In re Dulberg*, 129 USPQ 348 (CCPA 1961)). For example, Ginter et al. disclose separating the keys from the content ('900, figure 17). Regarding claims 1 and 17, however, a computer that differs from the prior art only in terms of data stored in memory wherein the data does not alter how the machine functions (i.e. non-functional descriptive material) will distinguish the claimed computer from the prior art in terms of patentability (MPEP 2100-22,23).

Claim 27 has been amended to recite "tagging the secret token to associate it with an application wherein the tag comprises the application's name". However, this is equivalent to "tagging the secret token with an application name", which is taught by Auerbach et al. (column 3/59-4/8). More specifically, Auerbach et al. teach cryptographic envelopes as executables, subroutines, modules or object components hence in order to be manipulated objects have to be defined or tagged.

Claims 18 and 34 have been amended to include the language of "wherein the stored encrypted serialized file enables the key and the key encryption key to be securely stored on a server." However, the Examiner maintains the 101 rejection as the outcome of the algorithm is mere storage. Further, the newly added language is described only in terms of what *can* be done (i.e. "enables", "to be securely stored") hence this language does further limit the method nor does it distinguish the method from the prior art (MPEP,

2100-8, "Language that suggests or makes optional but does not require steps to be performed or does not limit a claim to a particular structure does not limit the scope of a claim or a claim limitation.")

The following assertion of facts has gone unchallenged and are now considered admitted prior art:

- VPNs, SET, TLS and SSL are cryptographic technologies for forming a secure connection between computers communicating over a network
- serializing a software object for storing an object persistently

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

4. Claims 18-20 and 22-34 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 18 and 34 describe an algorithm. The "usefulness" of such an algorithm is not apparent, as the outcome merely results in the storage of a number or similar mathematical construct, and was produced without transformation of the data by a machine such as a computer. Hence the claimed invention does not produce useful, concrete and tangible result (*State Street*

Bank & Trust Co. v. Signature Financial Group Inc., 149 F.3d 1368, 1373, 47 USPQ2d 1596, 1600 (Fed. Cir. 1998)).

Claims 19-33 are also rejected as they depend from claim 18.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-9 and 11-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Auerbach et al., U.S. Patent No. 5,673,316 in view of Ginter et al. U.S. Patent No. 5,892,900 and Ginter et al. U.S. Patent No. 6,658,568.

As per claims 1-9 and 11-17, Auerbach et al. teach a network system for key management comprising:

- a server (figure 1; column 2, lines 11-15)
- a key management system providing process logic for key management system initialization located on the server, secure data

storage and an interface for providing a means for inputting data into key management system (figure 1; column 2, lines 11-15; column 9, lines 40-48) and using data to generate a key (column/line 4/65-5/8)

- a client computer, comprising a user interface (GUI or browser) for inputting data into the key management system, connected to the server (figure 1; column 1, lines 54-60; column 6, lines 50-61; column 8, lines 5-15; column/line 8/45-9/10)
- key management storage located on a server or on a second server connected to the server (figure 1; column 2, lines 10-15)

Auerbach et al. also disclose a randomizer for randomizing data, key generation tool for generating symmetric and asymmetric keys, and MD5 hashing functions (column/line 4/65-5/26). Regarding an encrypted connection between client and server, Auerbach et al. disclose a user purchasing content using an account number exchanged between client and server (column/line 6/67-7/5; column 8, lines 52-54). Auerbach et al. also disclose securing this exchange using standard cryptographic techniques (column 8, lines 58-62; column 10, lines 35-40). VPNs, SET, TLS and SSL are well known cryptographic technologies for forming a secure connection between computers communicating over a network, therefore it would have been obvious to one of ordinary skill to protect the user account number or credit card number as it travels from buyer to server (figure 1).

Auerbach et al. also teaches a memory in the key management system for storing data such as a key encryption key (column 5, lines 7-12) and encrypting module for encrypting data (column 6, lines 22-27), however they do not specifically recite a key management system that performs hashing of a key encryption key and creating a serialized file. Ginter et al. ('900) teach a system for secure content distribution (figures 1, 1A, 2, 5B and 79-82). Specifically, Ginter et al. ('900) teach a content seller (figures 79-82; column/line 63/65-64/15; column/line 86/63-87/18; column 112, lines 45-52; column/line 210/31-211/24) generating its own certificate using data from memory (e.g. CA private key, its own public/private key pair- column 211, lines 45-58; column 212, lines 5-10) so that a user can trust the seller and its public key (column/line 210/31-211/24). Neither Auerbach et al. nor Ginter et al. ('900) specify a type of certificate. Ginter et al. ('568) teaches a certificate for authorizing entities in a secure content distribution environment (figures 12, 13, 22, 22A, and 23; column 30, lines 30-40; column 84, lines 4-18) where the certificate includes data from memory, a hash of public key and encrypting (or encoding) (column 84, lines 10-15) or encrypted (or encoded) data (column 84, lines 18-21). Regarding "serializing data", "serialization" is a well-known method for storing an object persistently. Therefore, it would have been obvious to serialize an object such as a digital certificate, in order to reconstitute it at a later time such as when a prospective buyer would like to authenticate content seller. Therefore, it would have been

obvious to one of ordinary skill to combine the teachings of Auerbach et al., Ginter et al. and Ginter et al. in order to create a trusted electronic commerce environment by allowing the user to be able to authenticate the seller ('316, figure 1; '568, column 30, lines 30-40).

7. Claims 18-20 and 22-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Auerbach et al., U.S. Patent No. 5,673,316 in view of Havemose, U.S. Patent No. 6,757,903.

As per claims 18-20 and 22-35, Auerbach et al. teach:

- entering data and a key encryption key into a key management system (abstract)
- combining data into a tuple (e.g. document part and control part) (figure 2)
- encrypting the tuple (encoding a key field of the tuple) with the key encryption key to create a token (abstract; figure 2)
- hashing the encryption key (figure 3)
- storing the token in a vector (column/line 3/58-4/2)
- storing the hashed key (figures 2 and 3)
- storing a list of keys (figures 2 and 3)
- randomizing data (column 5, lines 1-8)
- randomizing the list of keys and secret tokens (figure 3)

- generating data to encrypt (abstract; figure 2)
- a tuple with an application, key, value and type field (figure 3)
- key management storage located on a server or on a second server connected to the server (figure 1; column 2, lines 10-15)
- a client computer, comprising a user interface (GUI or browser) for inputting data into the key management system, connected to the server (figure 1; column 1, lines 54-60; column 6, lines 50-61; column 8, lines 5-15; column/line 8/45-9/10)

Regarding "tagging" the method and system of Auerbach et al. is implemented using computer code (column/line 3/59-4/8). More specifically, Auerbach et al. teach cryptographic envelopes as executables, subroutines, modules or object components hence in order to be manipulated objects have to be defined (i.e. tag). Regarding algorithms, teach a key generation tool that comprises a symmetric algorithm (column 5, lines 1-8) and a key generation tool that comprise asymmetric algorithms, for example for encrypting and decrypting data exchanged by client and server (column 7, lines 30-42; column 8, lines 22-25 and 58-63; column 9, lines 40-48; column 10, lines 35-40). Auerbach et al. do not specifically recite "serializing" a cryptographic envelope. Havemose teaches a system for more efficiently processing data objects using serialization (column 6, lines 28-50). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Auerbach et al. and Havemose in order to more

efficiently distribute dynamic objects ('903, column 12, lines 40-60) (such as the cryptographic envelopes of Auerbach et al. ('316, figure 3)) by making them platform and architecture neutral ('316, column/line 1/20-2/1; column 3, lines 6-35).

Conclusion

8 **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

9. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (571) 272-6709. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (571) 272-6712.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

c/o Technology Center 3600

Washington, D.C. 20231

or faxed to:

(571) 273-8300 (for formal communications intended for entry and after-final communications),

or:

(571) 273-6709 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Calvin Loyd Hewitt II
Primary Examiner
March 26, 2008